

UNITED STATES DISTRICT COURT

for the
District of Massachusetts

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Motorola phone, Model # XT1921-2, IMEI:
359542090438837

Case No. 19-mj-4207-DHH

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A-1

located in the _____ District of _____ Massachusetts _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B-1

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

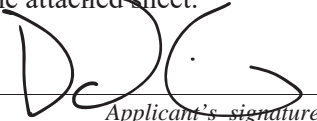
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1951(a)	Hobbs Act Robbery, and Conspiracy to Commit Hobbs Act Robbery
18 U.S.C. § 922(g)(1)	Felon in Possession of a Firearm

The application is based on these facts:

See Attached Affidavit of ATF Special Agent David Simmons

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

David Simmons, Special Agent, ATF
Printed name and title

Sworn to before me and signed in my presence.

Date: 03/19/2019

City and state: Boston, Massachusetts

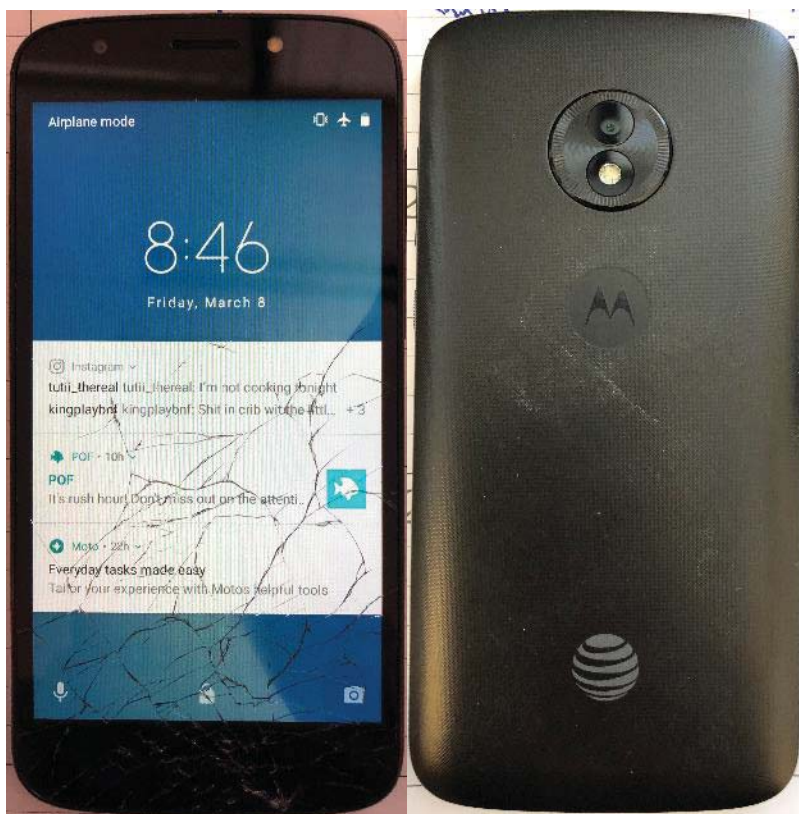

Judge's signature
Hon. David H. Hennessy, Chief U.S. Magistrate Judge
Printed name and title



ATTACHMENT A-1

The equipment to be searched consists of the following: Motorola phone, Model # XT1921-2, IMEI: 359542090438837 (“Target Device 1” or the “equipment”). Target Device 1 that is in possession of ATF, located at 1 Lakeshore Center, Bridgewater, Massachusetts 02324, as further described in Attachment A-1.

Images of the phone are included below:



ATTACHMENT B-1

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. §§ 922(g)(1), and 1951(a), including those related to:

- A. Communications, discussion, planning for and preparation of robberies, including selection of targets, familiarity with roads and means of access, procurement of transportation, procurement of weapons and ammunition, the disposition and monetization of stolen items;
- B. The identities, aliases, addresses, email addresses, whereabouts, and telephone numbers, of conspirators and other persons furthering the conspiracy;
- C. Possession of firearms and ammunition;
- D. The locations of meetings and other aspects of the conspiracy, including where the conspiracy was formed and was furthered, weapons and ammunition were obtained, the crime committed, and where suspects intended to flee;
- E. The methods of communications between conspirators and associates, including the telephone numbers, messaging applications, and social media accounts used by conspirators;
- F. The substance of communications regarding criminal activities, including discussions regarding firearms, ammunition, robberies, and any acts of violence;
- G. The identity, location, and travel or historical whereabouts of any conspirators or associates, as well as any acts taken in furtherance of the crimes listed above;
- H. Evidence of who used, owned, or controlled the equipment;
- I. Evidence of malicious computer software that would allow others to control the equipment, software, or storage media, evidence of the lack of such malicious

software, and evidence of the presence or absence of security software designed to detect malicious software;

- J. Evidence of the attachment of other hardware or storage media;
 - K. Evidence of counter-forensic programs and associated data that are designed to eliminate data;
 - L. Evidence of the times the equipment was used;
 - M. Passwords, encryption keys, and other access devices that may be necessary to access the equipment; and
 - N. Records relating to accounts held with companies providing Internet access or remote storage of either data or storage media.
- II. Serial numbers and any electronic identifiers that serve to identify the computer equipment.

DEFINITIONS

For the purpose of this warrant:

- A. “Equipment” means any hardware, software, storage media, and data.
- B. “Hardware” means any electronic device capable of data processing (such as a computer, digital camera, cellular telephone or smartphone, wireless communication device, or GPS navigation device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. “Software” means any program, program code, information or data stored in any

form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

- D. “Storage media” means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).
- E. “Data” means all information stored on storage media of any form in any storage format and for any purpose.
- F. “A record” is any communication, representation, information or data. A “record” may be comprised of letters, numbers, pictures, sounds or symbols.

Return of Seized Equipment

If, after inspecting seized equipment, the government determines that the equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy’s authenticity and accuracy (but not necessarily relevance or admissibility) for evidentiary purposes.

If equipment cannot be returned, agents will make available to the equipment’s owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, personally-identifying information of victims; or the fruits or instrumentalities of crime.